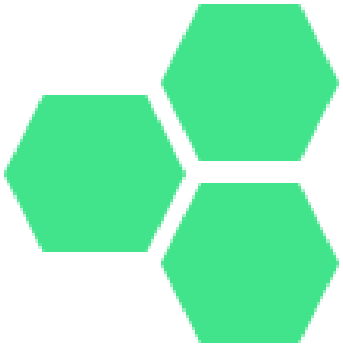
sproof

Discover sproof for

Managing Digital Documents



Abstract

sproof is a decentralized open source protocol, including applications to interact and to securely issue and verify digital documents. This process is made fast, easy and secure. Blockchain technology serves as a transparent registration service for both, issuers and digital documents. Verification of documents is completely free and available globally.

Challanges

Paper documents can be lost or stolen, easily forged and are hard to verify. This also holds for other types of certificates. While this can be improved by creating digital documents that can be digitally signed, there are still a number of yet unsolved challenges.

Verification

Verification of digital documents is hard and inconvenient. Each certificate needs to be checked individually and often requires to manually review the issuer. With sproof, this process becomes significantly easier. A high degree of automation and bulk-checking documents and issuers makes verification fast, easy and cheaper.

Revocation

Revocation of digital certificates requires the maintenance of one or more revocation lists. One or more of this lists or external escrow services need to be double checked for each documents. sproof simplifies this by having built-in revocation. The revocation of a certificate is an integral part of the sproof protocol and the state of a certificate can be easily check as part of the verification.

Decentralization

Documents are most commonly issued by a single institution and both, the verification and maintenance of these documents requires a to fully trust this institution. In sproof there is no single third party, escrow service or trusted entity. The sproof protocol and the sproof core are open source and can be used freely without of charge. Most importantly, data is never under control of sproof, but rather every user remains the sole owner of its data.

Actors

Issuer

Issuers are all kinds of institutes, companies or individuals, who want to securely issue a document to receivers.

- Easy integration in established systems
- Reduce costs for maintenance and issuing

Receiver

Receivers are all individuals, companies or institutes who need a publicly auditable certification.

- Carry tamper-proof documents in the pocket
- Authenticate fast, securely and independently of third parties

Verifier

Verifiers are companies or individuals who need to check and verify authentic information or identify persons via previously issued documents.

- Reduce costs to verify documents
- Automatic and bulk verification

Documents

Document are all kinds of digital information. This includes diplomas, membership cards, medical records, certificates of employment, insurance policies and much more.

Decentralization

Blockchain

sproof is designed independently of concrete or existing blockchain implementations. It works on top of all common blockchain implementations and is ready for future developments. The current implementation of the sproof core is build on top of Ethereum. The blockchain acts as a chronologically ordered public registry and lookup service for documents and for checking their validity.

Privacy

We value privacy. Issuing a document in sproof does not imply that the content, such as a name or grade, is publicly readable. Sensitive data is protected with state of the art cryptographic technologies.

Costs

sproof develops a public storage module to combine cheap storage of distributed hash tables with the power of blockchains. sproof uses the public storage module to lock a hash references of data in the blockchain and to store the raw data on a distributed hash table.

Scalability

The global data set needed to verify documents and issuers is built off chain. By using the sproof protocol there is no need to interact with the blockchain for each document to be issued. With sproof it is possible to issue multiple documents at once with a single blockchain interaction.

Layers

Application Layer

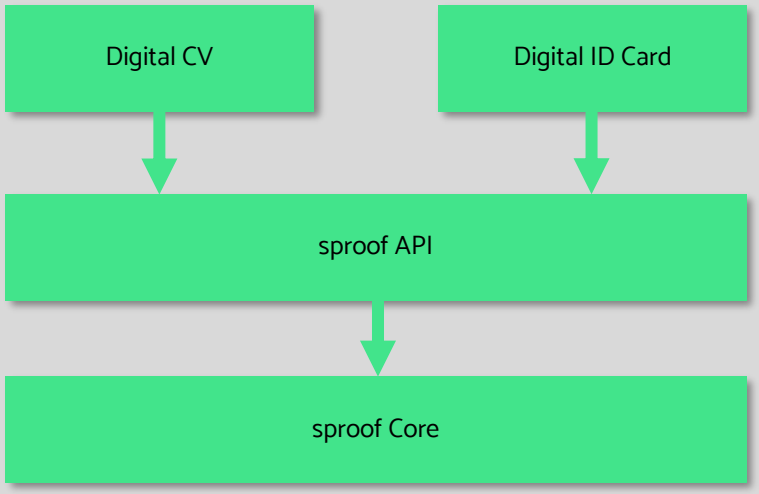
The application layer describes all application that interact with sproof and make use of the sproof service layer. Developers can create new applications based on the sproof open source protocol.

Service Layer

The service layer provides a standardized API calls for issuers and verifiers for an easy integration the sproof core layer for all kinds of processes and applications. This enables the feature that developers can integrate sproof in already established systems or to easily create new applications on top of the core layer.

Core Layer

The core layer defines the sproof protocol and the processes needed for registering and verifying issuers. Furthermore, sproof creates a consistent global state of all data stored in the public storage. The core layer is the main part of sproof.



Sproof Components

Sproof Node

The sproof node is open source and freely available. It provides the full sproof core, including a free API at the service layer for interaction with the sproof public dataset. A basic viewer at application level is additionally provided to view and verify documents and issuers.

Sproof Premium Services

To interact with the open source protocol developers need to host their own node and gather own cryptographic assets. The sproof premium services encapsulates this processes for issuers to allow easy interaction with the public storage hosted by sproof.

Sproof Webapp

sproof provides a webapp at the application layer for full and easy interaction with the sproof core module. The webapp can be used by small companies which does not have a build in software for issuing documents.

Sproof App

The sproof App allows receivers to collect and securely store their documents. App users can easily share and proof the ownership of a document with third parties who act as verifier.

Example Use Cases

The use cases of sproof are unlimited, the sproof API provides a generic interface to register and issue all kinds of digital assets. Here are a few examples of typical use cases for sproof.

Digital Identification

ID or membership cards are a perfect use case for sproof. Such cards can be used to automatically authenticate user for, i.e., a web login. sproof ID Cards can also represent a digital passport or a driving license issued by governments. sproof also enables features to authenticate card holder by biometric properties.

Intellectual property

sproof provides an API to register digital documents, describing a patent or an intellectural property. A decentralized and transparent timestamp for the registration of documents is obviously provided.

Digital Curriculum Vitae

For educational institutes or companies sproof can be used to issue a digital certificate that represents a diploma, additional trainings or certificates of employments. Receivers are able to create a digital CV with one click within seconds.

Team

Clemens Brunner, MSc

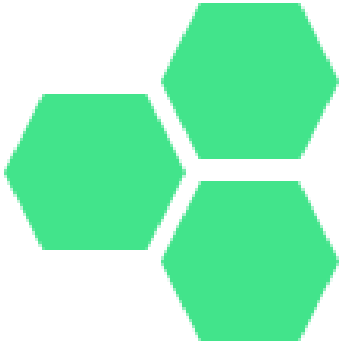
Clemens Brunner is a PhD student at the Computer Sciences Department at University of Salzburg since 2018 and a researcher at the Center for Secure Energy Informatics at Salzburg University of Applied Sciences since 2018. He received the Master's degree in 2017 from University of Innsbruck. His current research interest is on decentralized trust management systems and privacy preserving authentication.

Dr. Fabian Knirsch

Fabian Knirsch a researcher at the Center for Secure Energy Informatics at Salzburg University of Applied Sciences and co-founder of cappatec. He received his PhD in Computer Sciences in 2018 from the University of Salzburg. His research interest is currently on security and privacy and privacy enhancing technologies in the smart grid user domain.

Erich Höpoldseder

Erich Höpoldseder has successfully implemented innovations and business development processes in various markets for international companies for more than 25 years. He has excellent management, technical, sales and social skills and has filed several patents. He supports products that improve the quality of life of people and contribute to greater safety.



office@sproof.it

Contact us for further information and collaboration.